UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,537	02/09/2004	Brian Hernacki	SYMAP041	6706

21912 7590 11/12/2008

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
TRAN, TUNG Q	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
11/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,537	HERNACKI, BRIAN	
	Examiner	Art Unit	
	TUNG Q. TRAN	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-16 and 18-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-16 and 18-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 7-8 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 7-8 are claimed to be dependent on claim 6 but claim 6 has been cancelled. For purpose of examination in relation to the prior arts, Examiner will interpret that claims 7-8 are dependent on claim 1.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7-16 and 18-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pochon et al. (US 2003/0048793), of record, in view of Cantrell et al. (US 2004/0093513) and further in view of Hamadeh et al. (US 2004/0093521).

Regarding claims 1, 20, and 21, Pochon discloses a method for assembling fragmented network traffic, comprising: detecting in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed (¶¶ [0089]-[0093], esp. ¶ [0093], where an NIDS checks to determine whether there is a conflict between previously received fragments and a currently received fragment, i.e. check to determine if there is an anomaly, see also ¶¶ [0022]-[0026]); and performing further processing on the fragmented network traffic having the anomaly (¶ [0093], where the fragmented network traffic having the anomaly is discarded).

Pochon does not expressly disclose initiating in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; wherein performing further processing comprises determining configuration information associated with how the destination node is configured to reassemble overlapping fragments. Rather, Pochon discloses that in response to detecting an anomaly the fragments are discarded (¶ [0093]). Cantrell teaches, in a system for identifying anomalies in fragmented network traffic (¶ [0026]), that if a "suspicious" packet is identified, i.e. an anomaly is identified, then the packet is set aside for a more careful examination (¶ [0057]), where this permits the system to quickly identify suspicious packets at line rate and then take extra time to detect whether the suspicious packet is benign or malicious to permit the return of benign packets to the transmission line (¶

[0061], see also ¶ [0063]). In addition, Cantrell discloses that the more careful examination includes the use of expanded buffering (¶ [0065], where the more careful examination includes comparing a copy of the suspicious packet to various signatures to determine if the suspicious packet is malicious, see also ¶¶ [0026] and [0062]- [0065], which discloses that the intrusion detection system can consider all options). It is implicit that this "expanded buffering" includes the fragments since the fragments are used to reconstruct the data stream. Cantrell also discloses that performing further processing comprises determining configuration information associated with how the destination node is configured to process the packet (¶ [0065], where a database of information pertaining to the various machines on the network is located in the intrusion detection system, see also ¶¶ [0026] and [0062]- [0065], where the intrusion detection system determines all options and looks at various protocols when processing the packet). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to initiate, in response to detecting said anomaly, expanded buffering of fragments contained in the fragmented network traffic to allow a more careful examination of the suspicious packet to determine whether the packet is benign or malicious.

Pochon and Cantrell do not explicitly disclose how the destination is configured to reassemble overlapping fragments. However, Hamadeh discloses determining configuration information associated with how the destination node is configured to reassemble overlapping fragments (¶¶ [114-118] and Fig. 7, where configuration information related to reconstruction algorithm the destination is used to reconstruct

overlapping fragments is determined to form a set of IP addresses). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to determine configuration information associated with how the destination node is configured to reassemble overlapping fragments to be able to determine the source of an attack within few minutes of its launch and while the attack is still ongoing. Hence, the reconstruction for traceback provides real-time identification of the addresses of routers involved in the attack.

Regarding claims 2 and 18, Pochon in view of Cantrell and further in view of Hamadeh discloses that detecting an anomaly comprises determining that said two or more fragments overlap (Pochon: ¶¶ [0022]-[0026], see also Cantrell: ¶ [0026]).

Regarding claim 3, Pochon in view of Cantrell and further in view of Hamadeh discloses that determining that said two or more fragments overlap comprises reading a header value associated with one of the fragments (Pochon: ¶¶ [0091]-[0092]).

Regarding claim 4, Pochon in view of Cantrell and further in view of Hamadeh discloses that the header value comprises an offset value (Pochon: ¶¶ [0091]-[0092]).

Regarding claims 5 and 19, Pochon in view of Cantrell and further in view of Hamadeh discloses that detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments (Pochon: ¶¶ [0022]-[0026], see also Cantrell: ¶ [0026]).

Regarding claims 7 and 22, Pochon in view of Cantrell and further in view of Hamadeh does not expressly disclose that determining configuration information

comprises querying the destination node; however, Pochon in view of Cantrell does disclose that determining configuration information comprises gathering such information in any known ways (Cantrell: ¶ [0065]). Examiner takes official notice that querying a node is a known way to gather information on the node. As such, it would have been obvious to one of ordinary skill in the art at the time of the invention to query a destination node since this is a known way to gather information on a node.

Regarding claims 8 and 23, Pochon in view of Cantrell and further in view of Hamadeh discloses that determining configuration information comprises querying an information base (Cantrell: ¶ [0065]).

Regarding claim 9, Pochon in view of Cantrell and further in view of Hamadeh discloses that performing further processing comprises reassembling the fragmented network traffic (Pochon: ¶¶ [0039]-[0040]) to generate more than one variant of the reassembled data flow (Cantrell: ¶¶ [0026] and [0062]-[0065]).

Regarding claim 10, Pochon in view of Cantrell and further in view of Hamadeh discloses processing the anomaly to determine whether the fragmented network traffic is associated with a threat (Cantrell: ¶¶ [0065]).

Regarding claim 11, Pochon in view of Cantrell and further in view of Hamadeh discloses performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat (Cantrell: ¶ [0063]).

Regarding claim 12, Pochon in view of Cantrell and further in view of Hamadeh discloses discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat (Cantrell: ¶ [0063]).

Regarding claim 13, Pochon in view of Cantrell and further in view of Hamadeh discloses copying one or more fragments comprising the fragmented network traffic to a buffer (Cantrell: ¶ [0065], where it is implicit that the traffic is copied to a buffer).

Regarding claim 14, Pochon in view of Cantrell and further in view of Hamadeh discloses that performing further processing comprises sending an alert (Cantrell: ¶ [0063]).

Regarding claim 15, Pochon in view of Cantrell and further in view of Hamadeh discloses that performing further processing comprises determining whether the fragmented network traffic should be blocked (Cantrell: ¶ [0063]).

Regarding claim 16, Pochon in view of Cantrell and further in view of Hamadeh discloses that performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node (Cantrell: ¶ [0063]).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TUNG Q. TRAN whose telephone number is (571) 272-9737. The examiner can normally be reached on Mon-Fri: 7:30 am - 5 pm, off alternative Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kwang B. Yao can be reached on (571) 272-3182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kwang B. Yao/

Supervisory Patent Examiner, Art Unit 2416